
IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

MURAT SULJOVIC,

Defendant.

Case No. 2:20-cr-153

**PROTECTIVE ORDER
PERTAINING TO
CLASSIFIED INFORMATION**

Judge Jill N. Parrish

This matter comes before the Court upon the United States' Stipulated Motion for Protective Order to prevent the unauthorized use, disclosure, or dissemination of classified national security information and documents that will be reviewed by or made available to defense counsel in this case.

Pursuant to the authority granted under section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2006) ("CIPA"); the Security Procedures established pursuant to Pub. L. 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA § 9) (hereinafter the "Security Procedures"); the Federal Rules of Criminal Procedure 16(d) and 57; the general supervisory authority of the Court; and, in order to protect the national security, the Government's motion is GRANTED.

IT IS HEREBY ORDERED:

1. The Court finds that this case will involve classified national security information, the storage, handling, and control of which, by law or regulation, requires special security precautions, and access to which requires a security clearance and a need-to-know.

2. The purpose of this Protective Order ("Order") is to establish the procedures that must be followed by the attorney(s) of record for the defense and their approved employee(s), translator(s), and investigator(s) (collectively referred to hereinafter as "the Defense"), any court personnel, and all other individuals who receive access to classified information or documents in connection with this case.

3. The procedures set forth in this Order, CIPA and any other applicable statutes shall apply to all pretrial, trial, post-trial, and appellate aspects of this case and may be modified by further order of the Court acting under Federal Rules of Criminal Procedure 16(d), sections 3 and 9 of CIPA, , and this Court's inherent supervisory authority to ensure a fair and expeditious trial.

Definitions

4. As used herein, the terms "classified national security information and documents," "classified information," "classified documents," and "classified materials" refer to:

- a. Any classified document or information that has been classified by any Executive Branch agency in the interest of national security or pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL" or "SECRET" or "TOP SECRET" or any information contained in such documents;
- b. Any document or information, regardless of its physical form or characteristics, now or formerly in the possession of a private party, which has been derived from a United States Government classified document, information, or material, regardless of whether such document, information, or material has itself subsequently been classified by the Government pursuant to Executive Order 13526 or its predecessor orders as "CONFIDENTIAL" or "SECRET" or "TOP SECRET" ;
- c. Classified information known to the defense counsel; and
- d. Any document or information that defense counsel have been notified by the Government orally or in writing contains classified information.

5. The words "documents," "information," and "materials" shall include, but are not limited to, all written or printed matter of any kind, formal or informal, including originals,

conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise), and further include but are not limited to:

- a. Papers, correspondence, memoranda, notes, letters, reports, summaries, photographs, maps, charts and graphs, interoffice and intra-office communications, notations of any sort concerning meetings or communications of any kind, bulletins, teletypes, telegrams and telefacsimiles, invoices, and worksheets, as well as drafts, alterations, modifications, changes, and amendments of any kind to the foregoing;
- b. Graphic or oral records or representations of any kind, including but not limited to photographs, charts, graphs, microfiche, microfilm, videotapes, sound recordings of any kind, and motion pictures;
- c. Electronic, mechanical, or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes or disks, and all manner of electronic data processing storage; and
- d. Information acquired orally.

6. "Access to classified information" means having access to, reviewing, reading, learning, or otherwise coming to know in any manner any classified information.

7. "Secure Area" shall mean an area approved by a Classified Information Security Officer ("CISO") for storage, handling, and control of classified information.

Classified Information

8. All classified documents or material and the information contained therein shall remain classified unless the documents or material bear a clear indication that they have been declassified by the agency or department that is the originating agency (hereinafter the "Originating Agency") of the document, material, or information contained therein.

9. Any classified information provided by the Government to the Defense is to be used solely by the Defense to prepare a defense in this case. The Defense may not disclose or cause to

be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provide herein.

10. Classified Information Security Officer. In accordance with the provisions of CIPA and the Security Procedures, the Court designates Winfield S. “Scooter” Slade as the CISO and Debra M. Guerrero-Randall, Daniel O. Hartenstine, Joan B. Kennedy, and Maura L. Peterson as Alternate CISOs for the purpose of providing security arrangements necessary to protect from unauthorized disclosure any classified information to be made available in connection with this case. Defense counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

11. Government Attorneys. The Court has been advised that the Government attorneys working on this case, Assistant United States Attorneys Tyler M. Murray and Carl D. LeSueur and U.S. Department of Justice National Security Division Trial Attorney Michael J. Dittoe, or any other appropriately cleared personnel in the United States Attorney’s office, the National Security Division, and the Federal Bureau of Investigation, (collectively refereed to herein as as the "Government Attorneys"), have the requisite security clearances to have access to the classified information that relates to this case. All references to Government attorneys, or attorneys for the Government, as used in this Order, refer only to the attorneys listed in this paragraph and their respective supervisors.

12. Protection of Classified Information. The Court finds that, in order to protect the classified information involved in this case, only Government attorneys, appropriately cleared Department of Justice employees, personnel of the Originating Agency; defense counsel, employees of defense counsel, translators, and investigators employed or hired by defense counsel, shall have access to the classified information in this case. No defense counsel or

defense counsel employee, including any translator, shall have access to any classified documents and information in this case unless that person shall first have:

- a. Received permission of the Government or, where necessary, the Court through a separate Court order;
- b. Received the necessary security clearance at the appropriate level of classification, through or confirmed by the CISO; and
- c. Signed the Memorandum of Understanding in the form attached hereto, agreeing to comply with the terms of this Order.
- d. Defense counsel shall file originals of the executed Memoranda of Understanding with the Court under seal and serve copies of such documents upon the CISO and the Government.
- e. The substitution, departure, or removal for any reason, from this case of counsel for the defendant, or anyone associated with the defense as an employee or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

13. Defense Counsel. Subject to the provisions of this Order, the following attorney(s) for the defense and their approved employee(s), translator(s), and investigator(s) (collectively referred to hereinafter as "the Defense"), may be given access to classified information as required by the Government's discovery obligations: Jessica Stengel, and other attorneys or investigators in the Federal Public Defender's Office who have or will have received the appropriate security clearance. The court has been advised, through the CISO, that the defendant's counsel, Jessica Stengel, holds security clearances permitting her access to the classified information that counsel for the government intend to use and disclose pursuant to this order. Any additional person whose assistance the Defense reasonably requires may have access to classified information in this case only after obtaining from the Court an approval for access to the appropriate level of classification on a need-to-know basis and after satisfying the other requirements described in this Order for access to classified information.

14 : Unless they already hold an appropriate security clearance and are approved for access to classified information in this case, the Defense, including all persons whose assistance

the Defense reasonably requires, shall complete and submit to the CISO a Standard Form 86 ("Security Investigation Data for Sensitive Position"), attached releases, and "major case" fingerprints in order to obtain security clearances necessary for access to classified information that may be involved in this case. The CISO shall provide access to the necessary forms. The CISO shall take all reasonable steps to process all security clearance applications.

15. Secure Area of Review. The CISO shall arrange for an appropriately approved Secure Area for use by the Defense. The CISO shall establish procedures to assure that the Secure Area is accessible to the Defense during normal business hours, after hours, and on weekends, in consultation with the United States Marshals Service, and once the Defense is approved for such access. The Secure Area shall contain a separate working area for the Defense, and will be outfitted with any secure office equipment requested by the Defense that is reasonable and necessary to the preparation of the defense in this case. The CISO, in consultation with defense counsel, shall establish procedures to assure that the Secure Area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No documents or other material containing classified information may be removed from the Secure Area. The CISO shall neither reveal to the Government the content *of* any conversations she may hear among the Defense, nor reveal the nature of documents being reviewed by them, nor the work generated by them. In addition, the presence of the CISO shall not operate to waive, limit, or otherwise render inapplicable the attorney-client privilege.

16. Filings with the Court. Until further order of this Court, any motion, memorandum, or other document the parties file that counsel knows, or has reason to believe, contains classified information in whole or in part, or any document the proper classification of which counsel is unsure, shall be filed under seal with the Court through the CISO, or an appropriately cleared

designee of her choosing. Pleadings filed under seal with the CISO shall be marked "Filed In Camera and Under Seal with the Classified Information Security Officer" and shall include in the introductory paragraph a statement that the item is being filed under seal pursuant to this Order, but need not be accompanied by a separate motion to seal. The date and time of physical submission to the CISO or a designee, which should occur no later than 4:00 p.m. MST, shall be considered as the date and time of court filing. At the time of making a physical submission to the CISO or her designee, counsel shall file on the public record in the CM/ECF system a notice of filing. The notice should contain only the case caption and an unclassified title in the filing. The CISO shall arrange for prompt delivery, under seal, to the Court and opposing counsel (unless ex parte) any document to be filed by the parties that potentially contains classified information. The CISO shall promptly examine the document and, in consultation with representatives of the appropriate Government agencies, determine whether the document contains classified information. If the appropriate Government agency determines that the document contains classified information, the CISO shall ensure that the classified portions of the document, and only those portions, are marked with the appropriate classification markings, and that those classified portions remain under seal. Following such a determination by the appropriate Government agency, the CISO shall promptly unseal, and place in the public record, all portions of any document filed by a party that do not contain classified information.

17. Keeping of Records. The CISO shall maintain a separate sealed record for those pleadings containing classified materials and retain such record for purposes of later proceedings or appeal.

18. Access to Classified Information. The Defense shall have access to classified information only as follows:

- a. All classified information produced by the Government to the Defense, in discovery or otherwise, and all classified information possessed, created, or maintained by the Defense shall be stored, maintained, and used only in the Secure Area established by the CISO;
- b. The Defense shall have free access to the classified information made available to them in the Secure Area and shall be allowed to take notes and prepare documents with respect to those materials. However, the Defense shall not, except under separate Court order, disclose the classified information, either directly, indirectly, or in any other manner which would disclose the existence of such;
- c. The Defense shall not copy or reproduce any classified information in any form, except with the approval of the CISO, or in accordance with the procedures established by the CISO for the operation of the Secure Area;
- d. All documents prepared by the Defense (including, without limitation, pleadings or other documents intended for filing with the Court) that do or may contain classified information shall be transcribed, recorded, typed, duplicated, copied, or otherwise prepared only by persons who have received an appropriate approval for access to classified information and only in the Secure Area on equipment approved for the processing of classified information and in accordance with the procedures established by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, magnetic recordings, exhibits, etc.) containing classified information shall be maintained in the Secure Area unless and until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the Government;
- e. The Defense shall discuss classified information only within the Secure Area or in another area authorized by the CISO and shall not discuss or attempt to discuss classified information over any telephone instrument or communication system, including through electronic mail or the Internet;
- f. The Defense shall not disclose, without prior approval of the Court, any classified information to any person not authorized pursuant to this Order, including the defendant and defense witnesses. The Defense may disclose classified information to the Court, cleared court personnel, and the Government Attorneys who have been identified by the CISO as having the appropriate clearances and the need-to-know that information. Counsel for the government shall be given the opportunity to be heard in response to any defense request for disclosure to a person not named in this Order. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to this Order, and to comply with all terms and conditions of this Order. If the preparation of the Defense requires that classified information be disclosed to persons not named in this Order, then, upon approval by the Court, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel;

g. Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other Court order are granted access to the classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by the Defense to have such information confirmed or denied at trial or in any public proceeding in this case, the Defense must comply with the notification requirements of Section 5 of CIP A and all the provisions of this Order; and

h. In the event that classified information enters the public domain, the Defense is precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that the Defense had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. The Defense is not precluded from citing or repeating information in the public domain that counsel does not know or have reason to believe to be classified information, or derived from classified information.

19. Classified Information Procedures Act. Procedures for the use or disclosure of classified information by the Defense shall be those provided in sections 5 and 6 and 8 of CIP A. To facilitate the Defense's filing of notices required under section 5 of CIP A, the CISO shall make arrangements with the appropriate agencies for a determination of the classification level, if any, of materials or information, either within the possession of the Defense or about which the Defense has knowledge and which the Defense intends to use in any way at any pre-trial proceeding, deposition or at trial. Nothing submitted by the Defense to the CISO pursuant to this paragraph shall be made available to counsel for the Government unless so ordered by the Court or so designated by the Defense. Any and all items that are classified shall be listed in the defendant's CIPA section 5 notice. To the extent that any classified information is the basis of any motion filed by the Defense, such motion shall be preceded by a CIPA section 5 notice.

20. Violations of this Order. Unauthorized use or disclosure of classified information may constitute violations of United States criminal laws. In addition, violation of the terms of this Order shall be immediately brought to the attention of the Court and may result in a charge of

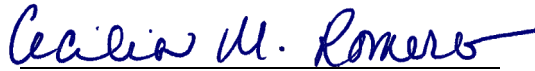
contempt of Court and possible referral for criminal prosecution. Any breach of this Order will result in the termination of a person's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized use, disclosure, retention, or negligent handling of classified information could cause serious damage, and in some cases exceptionally grave damage, to the national security of the United States, or may be used to the advantage of a foreign nation against the interests of the United States. This Order is to ensure that those authorized by the Order to receive classified information will never divulge the classified information disclosed to them to anyone who is not authorized to receive it or otherwise use the classified information without prior written authorization from the Originating Agency and in conformity with this Order.

21. All classified information to which the Defense has access in this case is now and will remain the property of the United States. The defense counsel, defense counsel employees, defense translators, defense investigators, and anyone else who receives classified information pursuant to this Order shall return all such classified information in their possession obtained through discovery from the Government in this case, or for which they are responsible because of access to classified information, to the CISO upon request. The notes, summaries, and other documents prepared by the Defense that do or may contain classified information shall remain at all times in the custody of the CISO for the duration of this case. At the conclusion of all proceedings, including any final appeals, all such notes, summaries, and other documents are to be destroyed by the Court Information Security Officer in the presence of defense counsel if so desired.

22. Nothing in this Order shall preclude the Government from seeking a further protective order pursuant to CIPA, and/or Rules 16(d) or 57 of the Federal Rules of Criminal Procedure, or any other applicable legislation as to particular items of discovery material.

23. A copy of this Order shall be issued forthwith to counsel for the defendants, who shall be responsible for advising their employees of the contents of this Order.

SO ORDERED this 21 day of June, 2021.



Cecilia M. Romero
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

vs.

MURAT SULJOVIC,

Defendant.

Case No. 2:20-cr-153

**MEMORANDUM OF
UNDERSTANDING REGARDING
RECEIPT OF CLASSIFIED
INFORMATION**

Judge Jill N. Parrish

Having familiarized myself with the applicable statutes, regulations, and orders, including but not limited to, Title 18 United States Code, sections 793, 794, 798, and 1924; the Intelligence Identities Protection Act, Title [50 U.S.C. Section 3121](#); Title [18 U.S.C. Section 641](#); Title [50 U.S.C. Section 783](#); and Executive Order 13526, I understand that I may receive information and documents that concern the present and future security of the United States. I understand that the material I receive belongs to the United States and that such information together with the methods and sources of collecting it remains classified by the United States Government. In consideration for the disclosure of classified information and documents:

(1) I agree that I will never divulge, publish, or reveal either by word, conduct or any other means such classified documents and information unless specifically authorized in writing to do so by an authorized representative of the United States Government or as expressly authorized by the Court pursuant to the Classified Information Procedures Act and the Protective Order entered by the court in the above-captioned matter.

(2) I agree that this Memorandum will remain forever binding on me.

(3) I have received, read, and understand the Protective Order entered by the United States District Court in the above-captioned matter relating to the handling of classified information, and I agree to comply with the provisions of that protective order.

(4) I understand that any prior contractual obligations that may bind me to continue to protect classified information remain in full force and effect and are not superseded by this Memorandum of Understanding. Additionally, I understand that this Memorandum of Understanding does not absolve me of any criminal or civil penalties that may otherwise be imposed upon me as a result of my unauthorized disclosure of classified information.

_____[Signed]
NAME [Printed]:
POSITION [Printed]:

Date